

UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*

Case No. 1:24MJ552

INFORMATION ASSOCIATED WITH
 tina97840@gmail.com STORED AT PREMISES
 CONTROLLED BY GOOGLE LLC

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 USC 922(d), 932(b)	Transfer of firearm to prohibited person; straw purchase attempt
18 USC 933(a)	Trafficking in firearms
18 USC 1001, 1512	False statements, witness tampering

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of 30 days *(give exact ending date if more than 30 days)*: _____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/S/ Cameron Winchester

Applicant's signature

Cameron Winchester, Special Agent, FBI

Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 12/10/2024


Judge's signature

City and state: Winston-Salem, North Carolina

The Honorable Joi E. Peake, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH
OF INFORMATION ASSOCIATED
WITH THE GOOGLE ACCOUNT
tina97840@gmail.com THAT IS
STORED AT PREMISES
CONTROLLED BY GOOGLE LLC

Case No. 1:24MJ552

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Cameron Winchester, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a “investigative or law enforcement officer of the United States” within the meaning of Title 18, United States Code, Section 2510(7). Specifically, I am a Special Agent for the Department of Justice, Federal Bureau of Investigation (DOJ/FBI). I have been a FBI Special Agent since October of 2022 assigned to the Raleigh/Durham Safe Streets Task Force (RDSSTF). Since becoming a Special Agent, I have investigated criminal street gangs and the trafficking of controlled substances. I have also received training in criminal investigations, violent gangs, illegal narcotics, physical surveillance, electronic surveillance, and preparing cases for prosecution. Prior to joining the FBI, I was employed as a Probation/Parole Officer with the North Carolina Department of Public Safety (NCDPS). In my role as a Probation/Parole Officer I supervised a gang caseload, worked violent crime, and fugitive matters. I was also assigned to NCDPS Special Operations and Intelligence

Unit and the FBI Raleigh/Durham Safe Streets Task Force (RDSSTF) of the Charlotte Field Office where I worked investigations into violent street gangs and narcotics distribution.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the Google LLC email accounts specifically described in **Attachment A** of this Affidavit, including tina97840@gmail.com ("TARGET ACCOUNT"). This information is stored at premises maintained, controlled, or operated by Google, an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 922(d) (knowing transfer of a firearm to a prohibited person), Section 932(b) (straw purchase attempt), Section 933(a) (trafficking in firearms), Section 1001 (false statements), and section 1512 (witness tampering), have been committed. There is also probable cause to search the information described in Attachment A for evidence of this crime as further described in Attachment B

3. The facts in this affidavit come from my personal observation, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. During my time as a Special Agent, I have conducted investigations of criminal matters involving use of the internet, social media, and other encrypted

communication platforms to further criminal activity. As a result of my experience in such investigations, I am familiar with the tactics, methods, and techniques of individuals, including the use of computers, cellular telephones and other forms of electronic communication to further their criminal activity. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of the statutes referenced above are contained within the TARGET ACCOUNT.

4. The following definitions apply to this Affidavit:

- a) "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a username or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish

communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and password.

- b) “IP Address” or Internet Protocol address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- c) “Computer” refers to an electronic, magnetic, optical, electrochemical, or other highspeed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e) (1).
- d) “Storage Medium” means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- e) “Computer hardware” consists of all equipment that can receive,

capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- f) “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it

inaccessible or unusable, as well as reverse the progress to restore it.

- g) "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- h) "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- i) "The Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- j) "Records" and "Information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
- k) The term "mobile device," as used herein, is defined as a small, hand-

held computing device, having a display screen, and an operating system (OS), with some type of input capabilities (such as a touch screen or a small keyboard), and is typically powered by a battery. Mobile devices are used to run various types of application software, known as “apps,” as well as communication functions allowing voice telephone calls, email communications, SMS and MMS functions. Cell phones, “Smart phones”, tablets, and PDAs are popular forms of mobile devices. Most handheld devices are often equipped with Wi-Fi, Bluetooth, and GPS capabilities, allowing the device to connect to the Internet and other devices (such as a vehicle or a microphone headset) or can be used to provide location-based services (like mapping and directional applications). Most mobile devices typically have an internal camera for taking and recording still image and video files, which are then stored within the memory of the mobile device or on a digital media storage device, like an SD card.

BACKGROUND CONCERNING GOOGLE¹

5. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web

¹ The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the “Google legal policy and products” page available to registered law enforcement at [lers.google.com](https://www.google.com/legal/enforcement/); product pages on support.google.com; or product pages on about.google.com.

browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

6. In addition, Google offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

7. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

8. Google advertises its services as “One Account. All of Google working for you.” Once logged into a Google Account, a user can connect to Google’s full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

9. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by

Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses (“recovery,” “contact,” “forwarding,” or “alternate” email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

10. Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts added by the user, as well as contacts the user has interacted with in Google products, up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

11. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their device calendar so it is stored in Google Calendar. Google preserves

appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

12. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

13. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to Google Drive. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google

Drive in a folder called “Shared with me.” Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

14. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

15. Google offers a cloud-based photo and video storage service called Google Photos. Photos and videos can be shared with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

16. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. Users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

17. Google collects and retains data about the location at which Google Account services are accessed from any mobile device. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History and Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

18. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history

and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

19. Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, likes, comments, and change history to posted videos. YouTube also may keep limited records of the IP addresses used to access particular videos posted on the service. Users can also opt into a setting to track their YouTube Watch History. For accounts created before June 2020, YouTube Watch History is stored indefinitely, unless the user manually deletes it or sets it to auto-delete after three or eighteen months. For accounts created after June 2020, YouTube Watch History is stored for three years, unless the user manually deletes it or sets it to auto-delete after three or eighteen months.

20. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive.

Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

21. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

22. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's

terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

23. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

24. In my training and experience, evidence of who was using a Google account and from where, as well as evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

25. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

26. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a

crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

27. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators or victims. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of additional victims and instrumentalities of the crimes under investigation.

28. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

PROBABLE CAUSE

29. On September 15, 2024, former President of the United States Donald J. Trump was golfing at Trump International Golf Club in West Palm Beach (Trump International), located at 3505 Summit Boulevard, West Palm Beach, Florida. At approximately 1:31 PM, a United States Secret Service (USSS) Special Agent assigned to the former President's security detail was driving a golf cart around the

perimeter of Trump International when the USSS Agent saw what appeared to be a rifle poking out of the tree line.

30. The Agent fired their service weapon in the direction of the rifle. A witness saw a male, later identified as RYAN ROUTH (ROUTH), fleeing the area of the tree line and entering a 2007, black Nissan Xterra, Florida license plate 97EEED. The witness then observed the same vehicle leave the area at a high rate of speed.

31. In the area of the tree line from which ROUTH fled, agents found a digital camera, two (2) bags, including a backpack, a loaded SKS-style, 7.62x39 caliber rifle with a scope and a round in the chamber, as well as a black plastic bag containing food. The serial number on the SKS-style rifle was obliterated and unreadable to the naked eye.



32. Officers from the Palm Beach County Sheriff's Office (PBSO) and the Martin County Sheriff's Office (MCSO) located the 2007 black Nissan Xterra as it traveled northbound on I-95. At approximately 2:14 PM, MCSO initiated a traffic stop

on the vehicle. The driver and sole occupant of the vehicle was ROUTH. ROUTH was asked if he knew why he was being stopped; he responded in the affirmative. The license plate attached to the 2007, black Nissan Xterra, Florida license plate 97EEED is registered to a different vehicle.

33. During the traffic stop, law enforcement transported the witness who had previously observed ROUTH fleeing the area of the Trump International tree line and entering the black Nissan Xterra. The witness identified ROUTH as the same individual he/she had previously seen entering the vehicle.

34. During a search of ROUTH's black Nissan Xterra, a Samsung phone, model A326U, was discovered (IMEI 351404590575402). During the analysis of this phone, law enforcement discovered correspondence between ROUTH and TINA COOPER, date of birth 02/07/1966, telephone number 336-904-5454. During the conversation, ROUTH and COOPER discussed the purchase of firearms.

35. The FBI Cellular Analysis Survey Team (CAST) analyzed the cellular location records associated with ROUTH's Samsung phone. The analysis determined that the device traveled from Greensboro, North Carolina to south Florida on August 14, 2024.

36. Between August 24, 2024 and August 30, 2024, ROUTH and COOPER exchanged text messages wherein ROUTH requested that COOPER assist him in procuring a different firearm and noted his inability to do so on his own, based on his prohibited status. These messages were discovered during the review of ROUTH's Samsung phone. During this time frame, ROUTH's Samsung phone communicated

exclusively with cellular towers located in Florida. There was no evidence in the cellular location records that ROUTH's Samsung phone left Florida.

TINA COOPER

37. On September 22, 2024, the FBI interviewed TINA COOPER at 1405 Fairview Street, Greensboro, North Carolina. COOPER advised she had known ROUTH since approximately 1999. COOPER had been an employee of ROUTH's at United Roofing in Greensboro, NC. COOPER and ROUTH maintained a professional and personal relationship from 1999 to 2004. COOPER was aware ROUTH had been charged with multiple felonies in 2002 after he threatened to blow up a police department. Additionally, COOPER believed ROUTH had plead guilty to approximately five felony charges in December of 2022; however, COOPER did not know if ROUTH had served any time in prison. COOPER lost contact with ROUTH in December of 2004 due to a disagreement between COOPER and ROUTH.

38. In approximately mid-July 2024, ROUTH called COOPER and advised he would be returning to Greensboro, North Carolina in approximately ten days and needed to purchase a firearm. ROUTH advised he needed to purchase the firearm for his son ORAN ROUTH (ORAN) for protection. COOPER recommended ROUTH purchase the firearm from a pawn shop, and ROUTH then reminded COOPER he was unable to purchase a firearm in his true name because he was a convicted felon. COOPER subsequently agreed to assist ROUTH with acquiring a firearm.

39. After agreeing to assist ROUTH with purchasing the firearm, COOPER reached out to RONNIE OXENDINE, date of birth 12/29/1963, and asked if he had

any firearms for sale. COOPER advised OXENDINE she wanted to purchase the firearm for ROUTH who intended to give the firearm to ORAN for protection. OXENDINE advised COOPER he was at the beach and did not have any firearms for sale. Around approximately July 27, 2024, ROUTH called COOPER and the two discussed the type of firearm ROUTH wanted. ROUTH advised he wanted a long-distance rifle similar to an AK-47. COOPER thought ROUTH's request was odd, but advised she may be able to find an equivalent firearm such as an SKS. During the conversation, ROUTH cautioned COOPER to be mindful what she sent via text message and explained his (ROUTH's) wife may be able to review their correspondence.

40. Following her conversation with ROUTH, COOPER again contacted OXENDINE and asked if he had an AK-47 for sale. During the conversation, COOPER and OXENDINE agreed on the sale and purchase of an SKS rifle. COOPER then requested that OXENDINE bring the SKS rifle to his business, Oxendine and Son's Roofing Company. On or about July 31, 2024, ROUTH called COOPER to inquire about the firearm she had agreed to help him acquire. COOPER advised she had not found an AK-47 for sale; however, she had found an SKS rifle for sale to which ROUTH advised would suffice and advised he wanted to proceed with the purchase.

41. COOPER advised that on August 2, 2024, she received a call from ROUTH who inquired about her location. COOPER advised ROUTH she was running errands with her daughter. COOPER called OXENDINE who confirmed he was at

Oxendine and Son's Roofing and had the SKS rifle with him. COOPER then called ROUTH and provided him the address to Oxendine and Son's Roofing.

42. COOPER and her daughter met ROUTH at Oxendine and Son's Roofing. OXENDINE was outside of the business when they arrived. OXENDINE questioned why ROUTH was present and was informed by COOPER that the rifle was actually for ROUTH instead of COOPER. ROUTH then gave OXENDINE \$350.00 for the SKS and gave COOPER \$100.00 for arranging the transaction.²

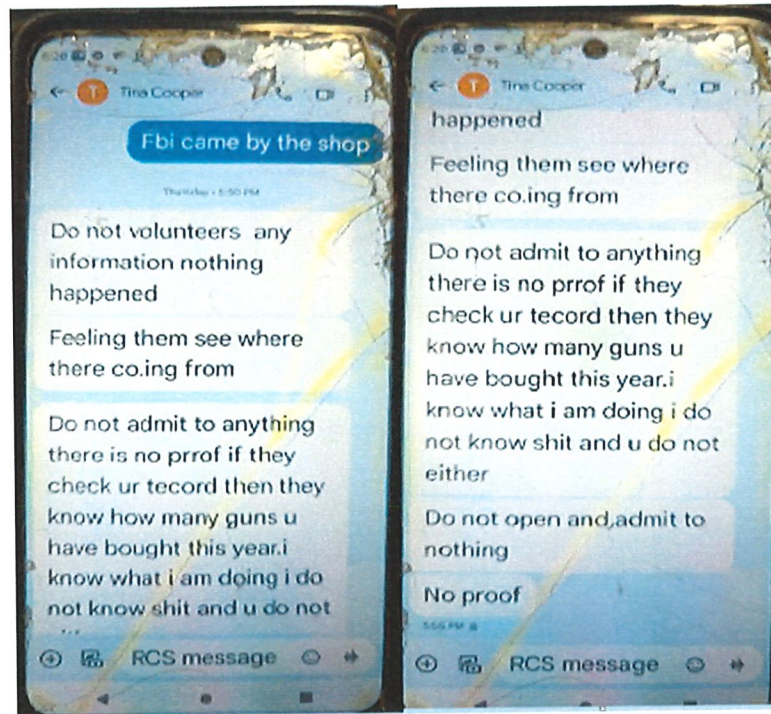
43. During the interview, COOPER consented to a review of her cellular telephone by the FBI. COOPER also advised she had deleted the contents of her telephone after she learned of ROUTH's attempted assassination of former President Donald J. Trump in West Palm Beach, Florida. COOPER further explained she deleted the content of the device to avoid any involvement with the assassination attempt.

44. A review of the device confirmed COOPER had deleted her call logs and text messages. Through reviewing COOPER's Facebook Messenger, agents discovered correspondence between COOPER and ROUTH from January 14, 2014, to January 1, 2022. During the interview COOPER provided multiple inconsistent stories to agents regarding the illegal firearms purchase between ROUTH, OXENDINE, and herself. COOPER was admonished and advised of 18 U.S.C. § 1001

² The FBI conducted multiple interviews of both COOPER and OXENDINE in relation to this firearms transaction. Some of the statements concerning the specific details of the sale were changed multiple times by COOPER and did not match OXENDINE's statement. The item of importance that appeared to your affiant to be consistent, and of relevance to the probable cause presented, is that the sale did occur and that COOPER brokered that sale.

(providing misleading for false statements to federal law enforcement). After this admonishment, COOPER admitted she lied to agents out of fear of criminal consequences for her involvement in the attempted assassination attempt of former President Donald J. Trump. Additionally, COOPER admitted she was “guilty” of assisting ROUTH, whom she knew was a prohibited person, in acquiring a firearm.

45. COOPER was asked if she had instructed any other person, involved in the aforementioned illegal firearms transaction, to lie to the FBI or mislead the FBI’s investigation in anyway. On multiple occasions, COOPER denied instructing anyone to lie to or mislead the FBI. COOPER was presented with text messages she sent to OXENDINE in direct contradiction of her statements to the FBI. After reviewing the messages, COOPER admitted to sending the text messages to prevent OXENDINE from cooperating with the FBI. The photograph below of text messages between COOPER and OXENDINE were discovered during a review of OXENDINE’s cellular telephone. The FBI had conducted an interview of OXENDINE on September 22, 2024. During that interview, OXENDINE consented to the extraction and review of his cellular telephone.



46. On October 17, 2024, the FBI Computer Analysis Response Team advised FBI Special Agent Cameron Winchester of the existence of the TARGET ACCOUNT, associated with COOPER's cellular telephone and discovered during the extraction thereof.

RONNIE OXENDINE

47. On September 22, 2024, the FBI interviewed OXENDINE at 3647 Randolph Church Road, Climax, North Carolina. OXENDINE advised he had met ROUTH in the early to mid-90's. OXENDINE and ROUTH both owned roofing companies and would occasionally cross paths at supply stores. OXENDINE and ROUTH were not friends. OXENDINE did not care for ROUTH and described ROUTH as being mouthy, arrogant, and obnoxious. OXENDINE advised ROUTH had pawned an SKS rifle with him in the early 90's for about \$300.00.

48. OXENDINE had learned of ROUTH's involvement with law enforcement from COOPER. OXENDINE knew ROUTH had been arrested in Greensboro, North Carolina for possession of weapons of mass destruction. Although OXENDINE knew ROUTH had been arrested, he did not know if ROUTH was ultimately convicted. OXENDINE also learned from COOPER that ROUTH had moved to Hawaii and gotten married. OXENDINE knew COOPER had worked for ROUTH's company in the early to mid-90's and may have been an owner in the company at some point.

49. OXENDINE advised that on August 2, 2024, COOPER called him and requested to purchase an AK-47. OXENDINE did not want to sell his AK-47 and instead offered to sell COOPER a SKS rifle. OXENDINE explained to COOPER that a SKS rifle shot the same round as an AK-47. OXENDINE believed COOPER was going to give the firearm to her grandson.

50. OXENDINE believed COOPER and ROUTH arrived at his shop located at 1702 Holbrook Street, Greensboro, North Carolina at approximately 10:00 am, on August 2, 2024. OXENDINE was surprised to see ROUTH; OXENDINE had not heard from ROUTH in approximately 10 years. OXENDINE asked why ROUTH was present and was advised the firearm was for ROUTH instead of COOPER. OXENDINE agreed to proceed with the sale. OXENDINE asked COOPER why she did not tell him the firearm was for ROUTH. COOPER advised she believed OXENDINE would have an issue with ROUTH being the recipient of the firearm.

51. After the initial conversation, OXENDINE handed the firearm directly to ROUTH. ROUTH paid OXENDINE \$350.00 and then paid \$100.00 to COOPER and thanked her. OXENDINE advised that he learned of ROUTH's attempted assassination of former President Trump from his sister. OXENDINE then contacted COOPER and advised her of ROUTH's assassination attempt of the former President. COOPER explained to OXENDINE she was going to delete all the messages with her and ROUTH. OXENDINE also explained COOPER had instructed him not to cooperate with the FBI.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

52. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

53. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time

convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

CONCLUSION

54. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

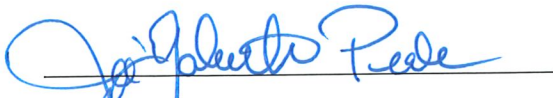
Respectfully submitted,

/s/ Cameron Winchester

Cameron Winchester
Special Agent
Federal Bureau of Investigation

On this day, the applicant appeared before me by reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

12/10/2024



The Hon. Joi E. Peake
United States Magistrate Judge
Middle District of North Carolina

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Gmail account **tina97840@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, LLC

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from **July 1, 2024 to September 22, 2024**:

- a. All business records and subscriber information, in any form kept, pertaining to the ACCOUNTS, including:
 1. Names (including subscriber names, usernames, and screen names);
 2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
 3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
 5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
 6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and
 8. Change history.
- b. All device information associated with the ACCOUNTS, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
 - c. Records of user activity for each connection made to or from the ACCOUNTS, including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs;
 - d. The contents of all emails associated with the ACCOUNTS, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;
 - e. Any records pertaining to the ACCOUNTS' contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;
 - f. Any records pertaining to the ACCOUNTS' calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;
 - g. The contents of all text, audio, and video messages associated with the ACCOUNTS, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication;

user settings; and all associated logs, including access logs and change history;

- h. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, [ANDROID USER: applications], and other data uploaded, created, stored, or shared with the account including drafts and deleted records; [ANDROID USER: third-party application data and backups]; [SMS data and device backups]; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;
- i. The contents of all media associated with the ACCOUNTS in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses;
- j. All maps data associated with the ACCOUNTS, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;
- k. All Location History and Web & App Activity indicating the location at which the ACCOUNTS was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history;
- l. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google

Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history;

- m. Records associated with the ACCOUNTS' YouTube registration, including the ACCOUNT's display name, IP logs, channel ID, account registration information, and registration email;
- n. The contents of all media associated with the ACCOUNTS on YouTube, whether active, deleted, or in draft, including: copies of videos and other media only if uploaded to, saved to, shared by or shared with the account; playlists; connected applications; associated URLs for each record; creation and change history; privacy settings for each record; and all associated logs, including IP addresses, locations, timestamps, and device identifiers;

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 922(d) (knowing transfer of a firearm to a prohibited person), Section 932(b) (straw purchase attempt), Section 933(a) (trafficking in firearms), Section 1001 (false statements), and section 1512 (witness tampering), for the account listed on Attachment A, in the form of the following:

- a. Records and information referencing the planning, attempt, brokering, or sale of firearms;
- b. Records and information referencing the knowledge or understanding of the intended use of the firearms sold or brokered;
- c. Records and information referencing knowledge of the purchaser of any firearms being a convicted felon or being a prohibited person;
- d. Records and information referencing the intent to destroy any evidence concerning the sale of firearms to a prohibited person;
- e. Records and information referencing the intent to corruptly influence the statements and/or testimony of witnesses concerning the sale of firearms to a prohibited person;
- f. Records and information referencing others involved in the offenses listed;
- g. Records and information revealing any other accounts used or accessed by the owner of the target accounts; and
- h. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s) at the time the records referenced above were generated or received.